

ABSTRACT OF THE DISCLOSURE

Disclosed is a security deciphering apparatus including a hidden secret key storing unit for storing a hidden secret key (K_h) corresponding to intrinsic identification information, a first decoding unit for receiving a personal secret key ($\{K_s\}K_h$), generated by enciphering a cipher key (K_s) by using the hidden secret key (K_h), via a public network, and decoding the personal secret key ($\{K_s\}K_h$) by using the hidden secret key (K_h), thereby obtaining the cipher key (K_s), and a second decoding unit for receiving enciphered data ($\{M\}K_s$), generated by enciphering data (M) by using the cipher key (K_s), via the public network, and decoding the enciphered data ($\{M\}K_s$) by using the cipher key (K_s), thereby obtaining the data (M). In accordance with the security deciphering apparatus, it is possible to receive data while maintaining a desired security of the data.